http://dx.doi.org/10.21544/2359-3075.30330

Tecnologías Cuánticas: una cuestión de soberanía nacional

Fernando M. Araújo-Moreira[1]
Vítor G. Andrezo Carneiro[2]
Juraci Ferreira Galdino[3]

RESUMEN

Los fundamentos de la física (o mecánica) cuántica fueron presentados por el científico alemán Max Planck en 1900. Con un contenido científico revolucionario, estos fundamentos establecieron nuevos paradigmas que respaldaron la llamada Primera Revolución Cuántica, de la cual derivaron productos como el láser, el GPS y los chips semiconductores, esenciales en la actualidad. En 1950, Chien Shiung Wu e Irving Shaknov llevaron a cabo lo que hoy se conoce como el experimento WS, que se convirtió en la clave para la manifestación emergente de la Segunda Revolución Cuántica. Esta incluye nuevas tecnologías agrupadas en cuatro grandes áreas: dispositivos cuánticos (sensores, biosensores, detectores y actuadores); comunicación y teletransporte cuánticos y materiales bidimensionales; computación, criptografía e internet cuánticas; y tecnologías derivadas de materiales cuánticos aplicadas, por ejemplo, al sector energético. Este artículo busca investigar indicios de que el campo de las Tecnologías Cuánticas es esencial no solo para la Seguridad y la Defensa Nacional, sino también para la configuración del tablero geopolítico. Se sugiere que, conjuntamente, las Tecnologías Cuánticas, la Inteligencia Artificial (IA) y la Cibernética impulsarán una gran revolución tecnológica para la humanidad y, particularmente, en los asuntos militares. Así, el artículo presenta argumentos para que estas áreas del conocimiento y desarrollo tecnológico sean consideradas estratégicas y prioritarias para el país, dado el papel central de estas tecnologías en el crecimiento económico, el desarrollo social, la seguridad, la defensa y la soberanía de una nación en el contexto de la 4ª Revolución Industrial y la Era del Conocimiento.

Palabras clave: tecnologías cuánticas; defensa cibernética; soberanía nacional.

[1] Ejército Brasileño. Instituto Militar de Ingeniería/Sección de Ingeniería Nuclear. Río de Janeiro, RJ, Brasil. https://orcid.org/0000-0002-5423-0405 http://lattes.cnpq.br/1809254923092721

[2] Ejército Brasileño. Instituto Militar de Ingeniería/Sección de Ingeniería Eléctrica. Río de Janeiro, RJ, Brasil. https://orcid.org/0000-0002-5738-168X http://lattes.cnpq.br/6739848742248437

[3] Ejército Brasileño. Instituto Militar de Ingeniería/Comando. Río de Janeiro, RJ, Brasil. https://orcid.org/0000-0001-7805-0452 http://lattes.cnpq.br/3588063339399737

> "Por lo tanto, digo que es una política limitada suponer que tal o cual país deba ser señalado como el aliado eterno o el enemigo perpetuo de Inglaterra. No tenemos aliados eternos ni enemigos perpetuos. Nuestros intereses son eternos y perpetuos, y es nuestro deber seguirlos."
> — Henry John Temple, 3.º Vizconde Palmerston

INTRODUCCIÓN

Las tecnologías cuánticas exploran fenómenos físicos probabilísticos que ocurren a escalas atómicas y subatómicas. La naturaleza probabilística de estos fenómenos fue tema del mundialmente famoso debate entre Albert Einstein y Niels Bohr, durante la Quinta Conferencia Solvay sobre Física Cuántica, celebrada en octubre de 1927 en Bruselas, cuyo principal objetivo era discutir la recién formulada teoría cuántica. Este evento reunió a 29 de las personas más prominentes de la época, de las cuales 17 se convirtieron en ganadoras del Premio Nobel.

En 1900, en lo que se conoció como el debate del siglo, Niels Bohr, uno de los padres de la teoría cuántica (de esencia probabilística) presentada por Max Planck, defendió la nueva teoría formulada por Werner Heisenberg, mientras Albert Einstein intentaba mantener un modelo de causa y efecto (es decir, esencialmente determinista). Einstein dijo: "Dios no juega a los dados" (refiriéndose al fenómeno probabilístico), a lo que Niels Bohr respondió: "Einstein, deja de decirle a Dios lo que debe hacer". Hoy en día, la comunidad científica está de acuerdo en que Bohr ganó el debate. Esto significa que el mundo, a escala cuántica, no tiene un escenario fijo basado en causa y efecto (determinismo), sino que es, de hecho, aleatorio. En otras palabras, se puede saber todo sobre el mundo atómico y subatómico sin saber exactamente qué ocurrirá a continuación. Esta concepción dio lugar a la llamada Primera Revolución Cuántica, que tuvo como resultados prácticos el desarrollo de muchos productos que, incluso hoy, tienen gran utilidad, tales como el láser, el GPS y los chips semiconductores.

El paradigma probabilístico permitió una mejor comprensión de algunas de las propiedades clave de las partículas atómicas y subatómicas, tales como el efecto túnel, la superposición y el entrelazamiento, así como

el dominio y avance de otras áreas aplicadas como la tecnología de la información, la nanotecnología y la mecánica de precisión. En 1950, Chien Shiung Wu e Irving Shaknov realizaron lo que hoy se conoce como el experimento WS, muchas veces citado como el primer experimento capaz de demostrar el fenómeno conocido como entrelazamiento cuántico. Junto con los fenómenos de túnel y superposición, este fenómeno cuántico se convirtió en la clave para el desarrollo de la Segunda Revolución Cuántica, que incluye nuevas tecnologías agrupadas en cuatro grandes áreas: dispositivos cuánticos (sensores, biosensores, detectores y actuadores); comunicación y teletransporte cuántico y materiales bidimensionales; computación, criptografía e internet cuánticas; y tecnologías derivadas de materiales cuánticos aplicables, por ejemplo, en el área energética.

Sistemas de comunicación con características muy avanzadas en cuanto a la seguridad de los datos y la velocidad de transmisión, un vasto conjunto de sensores con altísima sensibilidad y dispositivos de procesamiento de datos con velocidades que alcanzan Tb/s (terabits por segundo), son algunas de las posibilidades vislumbradas por los especialistas en lo que respecta a las innovaciones que podrían surgir a corto y medio plazo. Las emergentes Tecnologías Cuánticas podrían influir en la Seguridad y la Defensa Nacional, impactando fuertemente las futuras capacidades militares de las Fuerzas Armadas en todas las dimensiones de un moderno Teatro de Operaciones, dando lugar, según algunos autores, a la Guerra Cuántica, un nuevo paradigma para las crisis y los conflictos armados. Por lo tanto, los países que queden al margen de estos avances tecnológicos sufrirán enormes vulnerabilidades en su soberanía, además de obstáculos al crecimiento económico, científico y tecnológico y al desarrollo social.

Con todo esto, se puede percibir que los avances en tecnologías cuánticas tienen características disruptivas y deberán influir en varias expresiones del poder nacional, pudiendo volverse esenciales para el crecimiento económico, el desarrollo social y para la seguridad, defensa y soberanía de una nación. A pesar del alcance y la amplitud de las innovaciones derivadas de estas tecnologías, este artículo se centra en los desarrollos de estas innovaciones en el área de Defensa. Acompañar estos avances con un enfoque más técnico, particularmente en un área de difícil comprensión como la Cuántica, puede ser una tarea bastante problemática, especialmente en el área de Defensa, donde la divulgación de información siempre se realiza de forma protegida, cuando se realiza.

Así, este artículo busca realizar una prospección, con enfoque cualitativo y exploratorio, de las principales evoluciones en el área de Tecnologías Cuánticas, presentándolas de forma resumida y con base en la experiencia técnica de los autores en la implementación de algunas de estas tecnologías. En términos metodológicos, se llevó a cabo una amplia investigación bibliográfica en el área de Tecnologías Cuánticas, procurando presentar y organizar las referencias relacionadas con el uso de estas tecnologías para la Seguridad y la Defensa. Al enfocarse en tecnologías que actualmente se encuentran en desarrollo para un área tan sensible como la Soberanía Nacional, muchas veces tales referencias sólo se encuentran en breves noticias de revistas, correspondiendo al especialista tener una mirada más aguda para comprender los aspectos técnicos de lo que se está desarrollando.

Por lo tanto, este artículo pretende realizar un enfoque amplio en un mundo que atraviesa constantes transformaciones, especialmente en lo que respecta a los aspectos científicos, técnicos y geopolíticos relacionados con las tecnologías cuánticas de segunda generación y su influencia en las áreas de seguridad y defensa nacional en Brasil y en el mundo. Además, se presentan algunos de los nuevos paradigmas esencialmente ligados a las áreas de seguridad y defensa, así como se discuten las principales tendencias de algunas de estas tecnologías capaces de impulsar aún más la Cuarta Revolución Industrial y de desarrollar elementos esenciales de las capacidades militares de la Guerra del Futuro.

TECNOLOGÍAS CUÁNTICAS PARA LA SEGURIDAD Y LA DEFENSA NACIONAL

Promover la acumulación de capacidades tecnológicas, generar conocimiento y crear innovaciones en áreas sensibles y críticas, como las tecnologías cuánticas, es al mismo tiempo un gran desafío y una extraordinaria oportunidad para el crecimiento económico, el desarrollo social y la soberanía nacional de los países. Las tecnologías cuánticas deberán impactar fuertemente en todos los campos de la Expresión del Poder Nacional; sin embargo, es en la Expresión Militar donde se esperan los principales desarrollos, por las consecuencias previstas en todas las dimensiones del combate (terrestre, naval, aérea, espacial y cibernética), como se ilustra en la Figura 1.

Figura 1: Aplicaciones de las Tecnologías Cuánticas en la Defensa Nacional (adaptado de KRELINA, M., 2021).

Estas tecnologías no solo potencian las actuales, sino que también pueden crear capacidades militares poderosas e innovadoras, promoviendo una Revolución en los Asuntos Militares o incluso una Revolución Militar. Las expectativas de cambio son tan grandes que algunos autores incluso predicen el surgimiento de una nueva generación de la guerra: la Guerra Cuántica[5]. Otros consideran la cuántica no solo como una nueva generación de la guerra, sino también como una nueva dimensión del combate.

Según Krelina, la Guerra Cuántica (Quantum Warfare, en inglés) es aquella que utiliza tecnologías cuánticas para aplicaciones militares que afectan las capacidades de inteligencia, seguridad y defensa en todos los dominios de la guerra, introduciendo nuevas estrategias militares, doctrinas, escenarios y cuestiones de paz, así como dilemas éticos[3].

Las Tecnologías Cuánticas, entre otras posibilidades, permitirán medir o detectar objetos que hasta ahora eran indetectables con los paradigmas tecnológicos actuales, resolver problemas complejos que hoy no tienen solución y llevar las acciones cibernéticas a un nivel superior, tanto en términos de seguridad, con la criptografía cuántica, como en términos de procesamiento de datos, con la computación y los algoritmos cuánticos.

En el ámbito de la Seguridad y la Defensa, algunas aplicaciones merecen ser detalladas por su importancia y sus implicaciones a corto y mediano plazo[7]. A continuación, se abordan tres de las muchas Tecnologías Cuánticas con posibles aplicaciones en Seguridad y Defensa: dispositivos cuánticos, comunicación cuántica y computación cuántica.

Este artículo optó por centrarse en estas tres Tecnologías Cuánticas debido a que se encuentran en una fase más avanzada de desarrollo y por su enorme impacto, particularmente en el ámbito de la Cibernética, dado el alto grado de dependencia del mundo actual con respecto a los ordenadores. Sin embargo, el campo de la Cuántica presenta tantas características disruptivas que los autores no podían dejar de comentar sobre otros posibles impactos en la Seguridad y la Defensa.

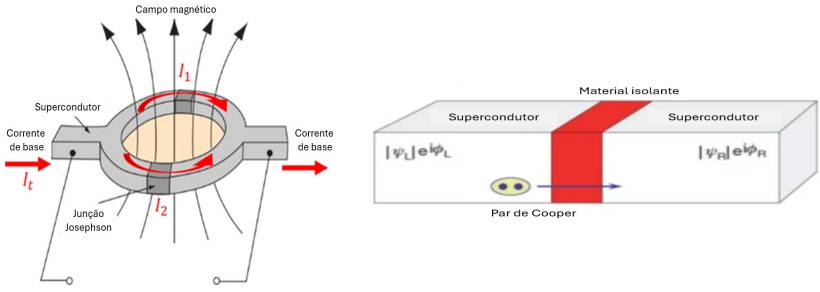
(a) Dispositivos Cuánticos

En este contexto, se discutirán los dispositivos de sensado cuántico, en particular sensores, biosensores, detectores y actuadores que utilizan los principios cuánticos de túnel cuántico, superposición y entrelazamiento, debido a su capacidad para medir magnitudes físicas con sensibilidades mucho más allá del límite clásico. Ya existen tecnologías de sensado comerciales que utilizan fenómenos cuánticos para alcanzar niveles extremadamente altos de precisión en la medición, incluyendo aplicaciones en relojes atómicos, resonancias magnéticas y paramagnéticas nucleares, y microscopios electrónicos.

Según la National Science Foundation (NSF), el equivalente estadounidense del CNPq, en los próximos diez años habrá varias oportunidades en términos de dispositivos cuánticos de última generación para aplicaciones en biotecnología y defensa, posicionamiento y navegación, y sistemas de cronometraje útiles tanto para las fuerzas armadas como para el sector civil. Al mismo tiempo, se abrirán nuevas oportunidades para abordar problemas complejos en ciencia de materiales, química y física. Estas aplicaciones tienen implicaciones significativas en áreas clave como la energía y la seguridad, impactando la vida cotidiana de la población en general.

Uno de los dispositivos cuánticos más importantes para el sensado es el llamado SQUID (Superconducting Quantum Interference Device), utilizado para medir campos magnéticos (Figura 2a). Está compuesto por una o más uniones de Josephson (Figura 2b). Uno de los aspectos más interesantes de esta unión es que constituye la base del bit cuántico (abreviado como qubit), utilizado en una de las estrategias tecnológicas para el desarrollo del ordenador cuántico. El qubit está formado por una partícula o propiedad física que asume un estado de superposición, lo que significa que puede representar los dos estados lógicos, 1 y 0,

simultáneamente. El estado (1 o 0) solo se define en el momento de la medición, y las estadísticas ocurren con una cierta probabilidad que depende del tipo de proceso que generó el qubit.



(a) (b)

Figura 2: (a) Esquema del sensor SQUID; (b) esquema de la unión Josephson.

Por ejemplo, en el área de la energía, las aplicaciones del sensado cuántico son bastante amplias, incluyendo energía renovable, energía nuclear, gestión de residuos nucleares, energía fósil, energía geotérmica, electricidad, electrificación de vehículos, etc. Las aplicaciones potenciales del sensado cuántico en áreas de energía fósil se muestran en la Tabla 1. Los diferentes tipos de sensores cuánticos se presentan en la Tabla 2.

Tabla 1: Aplicaciones potenciales del sensado cuántico en áreas de energía fósil.

Área de energia fóssil	Aplicação de sensoriamento
Utilização de CO2 e beneficiamento de carvão	Detecção rápida e sensível de emissão e vazamentos de CO2, detecção de metais de alto valor de carvão e subprodutos de utilização de carvão.
Upstream de Petróleo e gás	Gravímetros quânticos para a detecção de depósitos de petróleo / gás.
Midstream de Petróleo e gás	Monitoramento da integridade da tubulação durante o transporte e armazenamento.
Downstream de Petróleo e gás	Monitoramento da emissão de CO2 durante o consumo.
Captura e armazenamento de carbono	Detecção rápida e sensível de emissão de CO2 e vazamentos.
Extração e recuperação de carvão	Detecção de elementos metálicos críticos de carvão e subprodutos de utilização de carvão, gravímetros para exploração de carvão, segurança de minas de carvão.
Geração de eletricidade	Sensores que monitoram campos eletromagnéticos.
Transporte e distribuição de eletricidade	Monitoramento de temperatura em transformadores.
Física e energia nuclear	Monitoramento da segurança nuclear nacional, dispositivos de interferência quântica supercondutora (SQUIDs).

Tabela 2: Diferentes tipos de sensores quânticos e as tecnologias a eles associadas.

Tecnologia	Características quânticas	Condições experimentais	Vantagens vs. sistemas clássicos	Desafios
Sensores quânticos não fotônicos	Spin *qubits*, átomos neutros, íons presos	Medições de múltiplos parâmetros	Alta sensibilidade, baixo ruído	Decoerência, ruído de projeção quântica
Detecção remota de alvos	Iluminação quântica, emaranhamento quântico	Interferometria quântica	Relação sinal-ruído aprimorada	Muito frágil em relação à perda óptica
Radar quântico	Iluminação quântica de micro-ondas	Interferometria quântica	Expor alvos furtivos	Falta de conversores de fóton-micro-ondas
Espectroscopia quântica	Emaranhamento quântico, fótons únicos	Medições de correlação de intensidade	Além do limite de ruído de disparo, aproximando-se do limite quântico final	Decoerência quântica
Microscopia quântica	Emaranhamento quântico,	Microscopia e detecção quântica	Super resolução além do limite de Rayleigh	Localização desconhecida do centroide de origem
Interferômetros quânticos	Estados emaranhados, luz espremida	Interferômetros de menor escala	Escala de Heisenberg	Muito frágil em relação à perda óptica
Detector de ondas gravitacionais	Luz espremida	Interferômetros de tamanho quilômetro	Escala de Heisenberg	Muito frágil em relação à perda óptica
Leitura quântica da memória óptica clássica	Discriminação de canal quântico	Interferômetro e fonte de fóton único	Leitores ópticos mais rápidos e sem erros e memórias mais densas	Uso de fontes de fótons e detectores com altíssima eficiência

La Figura 3 muestra un resumen de las previsiones a diez años para el mercado de sensores cuánticos por tipo de sensor y las aplicaciones de estos sensores cuánticos.

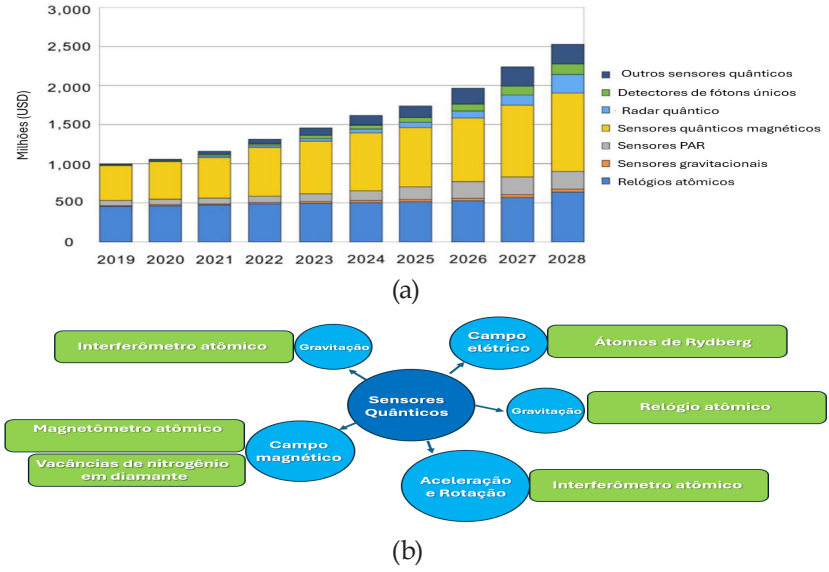


Figura 3: (a) Resumen de las previsiones a diez años para el mercado de sensores cuánticos por tipo de sensor; (b) aplicaciones de sensores cuánticos.

Específicamente, en el área de Seguridad y Defensa nacional, el sensado cuántico tendrá muchas aplicaciones en los diferentes teatros de operaciones y dominios del combate. Por ejemplo, podrá ser utilizado en la fabricación de sensores y detectores de explosivos y de agentes de guerra químicos, biológicos, radiológicos y nucleares. Los dispositivos cuánticos de PNT (del inglés, Position, Navigation and Timing) pueden ser utilizados como sistemas de navegación inercial confiables, permitiendo la navegación sin una referencia externa, como el GPS. Cuando se desarrolle completamente, este recurso podría ser revolucionario tanto para la navegación submarina como para plataformas terrestres.

Otra aplicación muy importante del sensado cuántico, con grandes implicaciones en el Teatro de Operaciones y que ya se encuentra en etapas intermedias de madurez tecnológica, es la detección, identificación y

estimación de PNT de submarinos y aeronaves furtivas. A continuación se presenta una pequeña muestra de la evolución en este sector.

A finales de 2023, el gobierno canadiense anunció la compra de 88 unidades del avión de combate considerado el segundo más moderno del mundo: el F35 Lightning. Fabricado por la estadounidense Lockheed Martin, el costo de la operación fue de aproximadamente 14 mil millones de dólares estadounidenses, es decir, el precio de cada unidad costó aproximadamente 160 millones de dólares (o 960 millones de reales por unidad). Este costo se justifica porque el F-35 Lightning tiene diversas características de última generación, como el motor más potente del mundo, fabricado por Pratt & Whitney; los modernos sensores que crean imágenes amplias del campo de batalla, permitiendo una mejor conciencia situacional, necesaria para la realización del C4ISR (sigla del inglés que significa, Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento); un sistema robótico avanzado llamado VLO Stealth, que tiene capacidad incomparable para detectar al enemigo e ingresar en el espacio aéreo disputado; posee un "Sistema de Guerra Electrónica", que detecta enemigos y bloquea radares. Debido a su sofisticación multifuncional, permite que el piloto opere en cualquier entorno y contra cualquier amenaza, pero la característica que lo diferencia de otros aviones de combate es su sigilosidad (también conocida como stealth mode, o simplemente stealth), es decir, su capacidad de ser invisible a los radares enemigos.

Sin embargo, la capacidad de sigilosidad del F35 y de otros aviones de combate tiende a volverse una tecnología obsoleta con el desarrollo de un sensor cuántico de última generación para actuar como radar, como ha anunciado China. La investigación y desarrollo de este radar comenzó en la última década... Actualmente, se supone que está en un nivel de madurez tecnológica (del inglés, Technology Readiness Level – TRL) superior a 6, lo que sugiere que podría hacer inviable las tecnologías de sigilosidad actualmente en uso. Este es uno de los casos demostrativos de ruptura de paradigmas en el área de Defensa debido a la producción de sensores cuánticos.

Los avances chinos en el sector son desafiados por los estadounidenses. El físico Jeffrey Shapiro, profesor del Instituto de Tecnología de Massachusetts (MIT) y pionero de la idea del radar cuántico, opinó que aún existen muchos desafíos tecnológicos que deben superarse para que el radar sea eficaz. Por otro lado, China Electronics Technology

Group Corporation (CETC) reveló un prototipo afirmando que podría identificar aeronaves furtivas en vuelo. Además, los científicos chinos explicaron que partículas cuánticas de alta energía serían capaces de detectar objetivos no visibles para los radares convencionales. A pesar de la guerra de narrativas, se debe tener en cuenta que los investigadores chinos afirman haber demostrado el efecto de detección furtiva, con objetivos a distancias significativas y, principalmente, los demostradores tecnológicos que se están presentando en China.

Figura 4: YIC-8E, el primer radar cuántico anti-stealth del mundo, creado por China.

Demostrando su capacidad tecnológica en el sector, China presentó recientemente un radar revolucionario en el Zhuhai Airshow: el YLC-8E. Este radar cuántico, que ha sido desarrollado por China (Figura 4), utiliza fotones de microondas entrelazados como método de detección y, al menos en principio, podría anular la tecnología stealth de los llamados aviones invisibles. Este desarrollo es considerado un gran desafío para los avanzados aviones de combate F-35 y F-22 de los EE. UU.

Figura 5: Imágenes del nuevo dron sigiloso ruso S-70.

Otro ejemplo demostrativo de los avances en la aplicación de dispositivos cuánticos en el área de defensa es el dron de ataque superpesado ruso (S-70 de Sukhoi-MIG), llamado Okhotnik (o Cazador), mostrado en la Figura 5. Este dron fue empleado experimentalmente en 2019, tiene un peso de 20 toneladas y una autonomía de 6.000 km, pudiendo alcanzar

una velocidad máxima de 1.000 km/h. Sus características operacionales de invisibilidad (grado de sigilo) y alta capacidad de sensorización indican el posible uso de sensores cuánticos, dada su alta sensibilidad y precisión.

Figura 6: Bombardero supersónico Stealth chino, H20.

El H-20, el nuevo bombardero supersónico chino (Figura 6), presentado durante las dos sesiones del Congreso Nacional del Pueblo, es otra innovación importante que sugiere la elevada capacidad tecnológica de China en tecnologías cuánticas, particularmente en dispositivos cuánticos. En una entrevista concedida al Hong Kong Commercial Daily en marzo de 2024, Wang Wei, subcomandante de la Fuerza Aérea del Ejército Popular de Liberación, reveló que el H-20 será anunciado oficialmente pronto al público, y negó que existan cuellos de botella técnicos, diciendo que el H-20 "es algo de lo que sentirse orgulloso y emocionado". El significado de este desarrollo es grande. Una de las características del H-20 es la cantidad de dispositivos cuánticos de sensorización y detección tanto a bordo como en los equipos de ataque.

(b) Comunicación Cuántica

Actualmente, se busca garantizar la seguridad de los datos en las comunicaciones civiles y militares mediante técnicas como la criptografía y el salto de frecuencia, esta última afecta más a las comunicaciones militares. Esto ocurre tanto en las comunicaciones confinadas, como las que utilizan fibra óptica, por ejemplo, como en las no confinadas, tales como las comunicaciones inalámbricas comúnmente utilizadas en los

Teatros de Operaciones mediante radios militares de comunicaciones tácticas. En el entorno de red, también se emplea el intercambio de claves criptográficas para hacer las comunicaciones más seguras.

Sin embargo, estos sistemas de comunicación convencionales explotan fenómenos electromagnéticos que son vulnerables a interferencias, interceptaciones y acciones de hackers, los cuales pueden copiar bits en tránsito sin dejar rastros. El nuevo paradigma de las comunicaciones cuánticas permite preservar la confidencialidad durante la transmisión.

Por otro lado, la comunicación cuántica aprovecha las leyes de la física cuántica para proteger la información. Estas leyes permiten que las partículas – normalmente fotones de luz – asuman un estado de superposición, formando el qubit de comunicación. Desde el punto de vista de la ciberseguridad, cuando un hacker intenta invadir el sistema mientras estos datos están en tránsito, el estado del qubit se altera, dejando un rastro de su invasión. Así, un hacker no puede manipular los qubits sin dejar una señal reveladora de su actividad.

Como consecuencia, se están llevando a cabo muchas investigaciones con el objetivo de crear redes de transmisión de datos altamente sensibles basadas en un proceso llamado Distribución de Claves Cuánticas (Quantum Key Distribution - QKD) que, en teoría, son ultra seguras. En este proceso, las propiedades cuánticas de ciertas partículas se utilizan para generar una clave secreta, que solo es conocida por las dos partes interesadas en comunicarse. El fotón fue la partícula física que se convirtió en la candidata natural para la implementación de los qubits en las comunicaciones cuánticas. Como normalmente se transporta a través de fibras ópticas o enlaces FSO (Free-Space Optics), ha aumentado la importancia de los grupos de investigación de todo el mundo que trabajan en fotónica o óptica cuántica.

El secreto del QKD está en las claves criptográficas, que se crean y transmiten en forma de qubits, por lo tanto, con gran seguridad. Sin embargo, las claves creadas se utilizan para cifrar los datos de manera clásica. En uno de los enfoques de QKD, el Protocolo BB84, cuyo nombre proviene de sus creadores (Charles H. Bennett y Gilles Brassard) y del año en que fue propuesto (1984), uno de los extremos crea la clave y la envía por un canal óptico. Luego, ambos extremos comparan una parte de sus claves, lo que se conoce como refinamiento de clave, para verificar si poseen la misma clave. Además, otro proceso conocido como destilación de claves puede detectar si la clave ha sido interceptada por un hacker. Si

esto ocurre, la clave es descartada y se generan nuevas hasta que se tenga la certeza de que una clave segura ha sido compartida

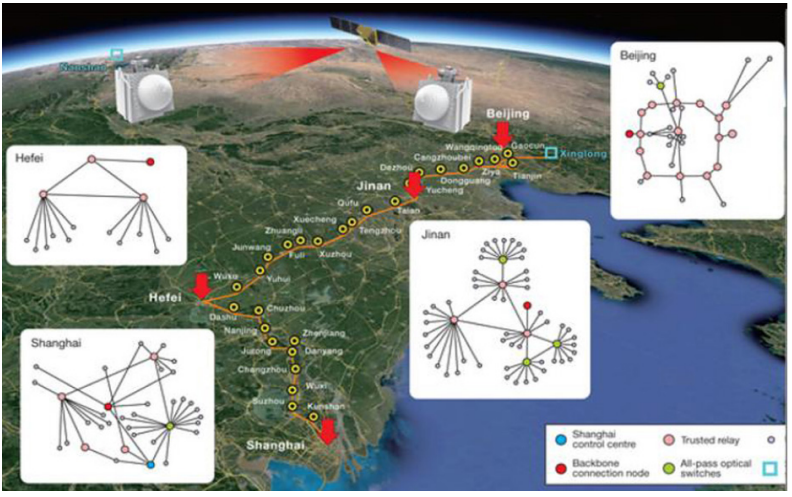


Figura 7: Red de comunicación QKD entre Pekín y Shanghái.

China ha demostrado avances sucesivos en el desarrollo de las comunicaciones cuánticas. En 2016, China lanzó los primeros satélites de comunicación cuántica, que utilizaban enlaces FSO para establecer una comunicación QKD entre dos estaciones terrestres separadas por 2.600 km. En 2017, ya existía una red de comunicación cuántica, con más de 2.000 km, entre Pekín y Shanghái, a través de enlaces de fibra óptica, con varios repetidores y dos satélites para apoyar la generación y transmisión de las claves cuánticas (Figura 7). En 2021, los investigadores ya habían aumentado el alcance máximo de un enlace QKD puramente terrestre a más de 500 km, utilizando una tecnología conocida como QKD de campo doble (TF-QKD).

A pesar de estos avances, aún hay mucho espacio para la investigación en redes de comunicación cuántica. Por ejemplo, el canal de comunicación cuántica puede ser ruidoso o tener imperfecciones que generen errores. Tales errores pueden confundirse como si fueran causados por la presencia de un espía, lo que hace que las claves generadas sean descartadas.

Otro problema a estudiar son los repetidores cuánticos, necesarios para redes de larga distancia. La red Pekín-Shanghái utiliza unos 30 repetidores, llamados nodos confiables, donde las claves cuánticas se

descifran en bits para luego ser retransmitidas cuánticamente. Un hacker que invada estos nodos podría copiar los bits sin ser detectado.

Con el objetivo de mitigar estos riesgos, algunos investigadores trabajan con otro tipo de enfoque, conocido como teletransporte cuántico. Esta tecnología se basa en la creación de pares de fotones entrelazados, que son transmitidos a ambos extremos del canal. Siempre que una interacción posterior cambie el estado del fotón entrelazado de uno de los extremos, el estado del fotón del otro extremo también se ve alterado debido al entrelazamiento cuántico. Para esto, no se necesita un canal cuántico. Solo es necesario un canal clásico que transmita el resultado de la medición realizada por el transmisor. Sin embargo, crear una red de teletransporte con muchos nodos sigue siendo un gran desafío. Investigadores de todo el mundo están buscando formas confiables de producir fotones entrelazados, a gran escala, bajo demanda y manteniendo su entrelazamiento a grandes distancias.

En 2015, un estudio publicado demostró el teletransporte de dos estados cuánticos del fotón, su espín y su momento angular. Ambos fueron usados como qubits. En 2017, el satélite Micius de China fue utilizado para teletransportar dos fotones entre Austria y China, en un experimento de comunicación cuántica de 7.600 km.

Notablemente, China es el país más avanzado en esta tecnología (Figura 8). En 2022, este país estableció un canal de Comunicación Directa con Seguridad Cuántica (QSDC) de 102,2 km, alcanzando el nuevo récord para este tipo de comunicación. El récord anterior para este tipo de canal era de 18 km. Un canal QSDC realiza tareas diferentes a un sistema QKD, ya que se crea un canal cuántico para la transmisión segura y confiable, tanto en relación con el ruido como con las escuchas. Usualmente, la creación de este canal seguro implica la generación de fotones entrelazados.

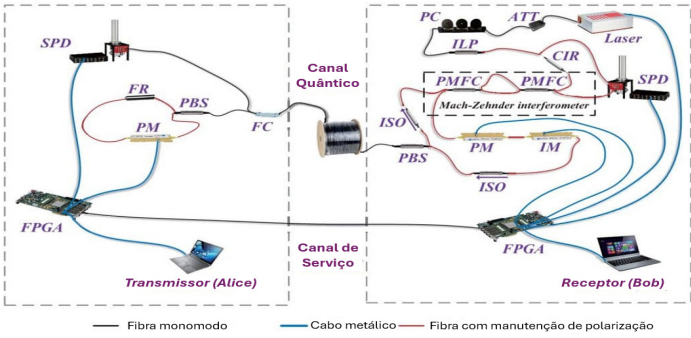


Figura 8: Red creada por China rompiendo el récord de distancia de QSDC (adaptado de ZHANG, H. et al., 2022).

No ámbito de la defensa en Brasil, destaca el proyecto liderado por el Instituto Militar de Ingeniería (IME), cuya ejecución cuenta con la colaboración de otros centros de investigación de Brasil, para también proponer un modelo de comunicación cuántica, basado en la generación y distribución de fotones entrelazados. Denominado Red Hermes Cuántica (RHQ), el proyecto tiene como objetivo inicial establecer una red de tres nodos entre el IME, la ECEME (Escuela de Comando y Estado Mayor del Ejército) y el CBPF (Centro Brasileño de Investigaciones Físicas) (Figura 9a). En esta red, se establecerá un protocolo QKD, basado en entrelazamiento y enlaces FSO.

(a) (b)

Figura 9: (a) Red Hermes Cuántica (RHQ): las líneas rojas representan los enlaces del IME hacia la Escuela de Comando y Estado Mayor del Ejército (ECEME) y hacia el Pan de Azúcar; la línea azul muestra el enlace del IME hasta el Centro Brasileño de Investigaciones Físicas (CBPF); (b)

Red Río Cuántica (RRQ) con su extensión.

Este proyecto estratégico para las Fuerzas Armadas cuenta con el apoyo del CBPF, la UFF (Universidad Federal Fluminense), la PUC-Rio (Pontificia Universidad Católica de Río de Janeiro) y la UFRJ (Universidad Federal de Río de Janeiro) en su ejecución. Otro socio importante es la UFPE (Universidad Federal de Pernambuco), cuyo Departamento de Física está trabajando en el desarrollo de dispositivos cuánticos necesarios para la computación y comunicación cuántica de extremo a extremo, sin necesidad de repetidores de señales que empleen el paradigma convencional. Los resultados de las investigaciones de la UFPE son esenciales para las próximas fases de la RHQ, en las que se prevén enlaces de fibra óptica de larga distancia. El IME firmó en marzo de 2024 un Acuerdo de Cooperación Técnica con la UFPE, y esta institución es una de las socias en la RHQ.

La RHQ es sinérgica y complementaria a otro importante proyecto realizado por las mismas instituciones: la Red Río Cuántica (RRQ), un emprendimiento liderado por la UFF. El principal objetivo de este proyecto es establecer una red metropolitana de comunicación cuántica, conectando estas instituciones con el IME. Algunos de los enlaces se extienden por decenas de kilómetros a través de fibra óptica. También se prevé un enlace aéreo de aproximadamente 7 km cruzando la Bahía de Guanabara (Figura 9b).

(c) Computación Cuántica

Los primeros pasos para el desarrollo de la computación cuántica comenzaron en la década de 1950. En 1981, durante una conferencia en el MIT, uno de los padres de la mecánica cuántica moderna, el físico Richard Feynman, presentó una propuesta para la utilización de sistemas cuánticos en computadoras, que tendrían entonces una capacidad de procesamiento superior a la de las computadoras convencionales. En 1985, David Deutsch, de la Universidad de Oxford, describió la primera computadora cuántica como una Máquina de Turing Cuántica.

Después de Deutsch, no fue hasta 1994 que hubo noticias de la computación cuántica, cuando en Nueva Jersey, en los Bell Labs de AT&T, el profesor de matemáticas aplicadas Peter Shor desarrolló un algoritmo (Algoritmo de Shor), capaz de factorizar grandes números a

una velocidad mucho mayor que la de las computadoras convencionales (clásicas). En 1996, Lov Grover, también de Bell Labs, desarrolló el Speedup, el primer algoritmo para la búsqueda en bases de datos cuánticas. En 1999, se construyeron en el MIT los primeros prototipos de computadoras cuánticas basadas en principios térmicos. La Figura 10 muestra el elemento principal de una computadora cuántica: el chip que almacena los qubits.

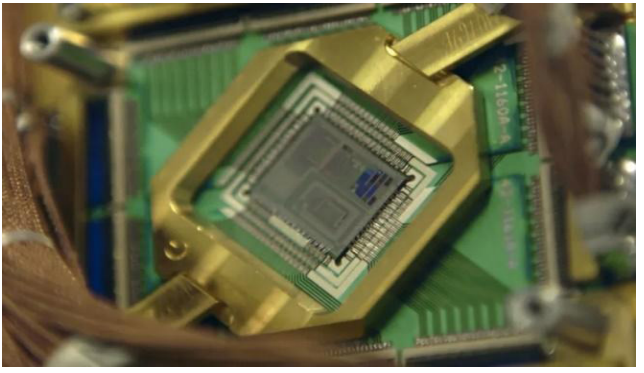


Figura 10: Elemento principal de una computadora cuántica: el chip que almacena la estructura de qubits.

En el año 2007, surgió el Orion, un procesador cuántico de 16 qubits que realiza tareas prácticas. Fue desarrollado por la empresa canadiense D-Wave Systems, basado en principios de superconductividad. En 2011, esta empresa lanzó el primer ordenador cuántico comercial llamado D-Wave One, con un procesador de 128 qubits. Sin embargo, el D-Wave One aún no era totalmente independiente y necesitaba ser utilizado junto con computadoras convencionales. En 2017, la misma empresa lanzó comercialmente el D-Wave 2000Q, un ordenador cuántico de 2000 qubits con un precio de 15 millones de dólares. Actualmente, D-Wave ya tiene ordenadores cuánticos con más de 5000 qubits. A pesar de que la cantidad de qubits ya no es un factor determinante en la evolución de un ordenador, ya que los chips más modernos están invirtiendo en la calidad y un mayor control de los qubits, los 5000 qubits representan un hito en el desarrollo. La Figura 11 muestra los principales actores mundiales en el área de fabricación de ordenadores cuánticos y el tipo de qubit utilizado para su desarrollo.

Tipo de *qubit*	Fabricante
Supercondutor	Google, IBM Q, rigetti, IQM, QuTech, qci, OQC, 本源量子
Íons aprisionados	IONQ, AQT, QUANTINUUM, oxford ionics, Universal Quantum
Fotônicos	PsiQuantum, XANADU, QUIX QUANTUM, ORCA Computing
Átomos neutros	ColdQuanta, QuEra COMPUTING INC., atom computing, PASQAL
Silício Spins/Quantum dots	intel, Silicon Quantum Computing, diraq, QUANTUM MOTION, QUANTUM BRILLIANCE

Figura 11: Principales actores mundiales en el área de fabricación de ordenadores cuánticos y el tipo de qubit utilizado para su desarrollo.

Entre las innumerables posibilidades vislumbradas para la aplicación de la computación cuántica, una merece destacarse: la factorización de números enteros. Esta es una clase de problema matemático que los ordenadores clásicos tardan un tiempo extremadamente largo en resolver (del orden de miles de millones de siglos), mientras que los cuánticos pueden resolverlo con eficiencia en pocas horas.

En la teoría de números, la factorización de enteros es la descomposición de un número compuesto en un producto de números enteros menores. Si esos factores se limitan a los números primos, por ejemplo, el proceso se denomina factorización prima. A pesar de ser un problema muy antiguo, la factorización de grandes números enteros aún no ha sido resuelta de manera eficiente. El interés en encontrar una solución para este problema aumenta cada vez más, ya que la seguridad de los actuales métodos de criptografía de clave pública, como el RSA (acrónimo compuesto por las primeras letras de los apellidos de Ron Rivest, Adi Shamir y Leonard Adleman), depende de la eficiencia actual de los métodos de factorización. Cuando los números son lo suficientemente grandes, no se conoce ningún algoritmo eficiente de factorización de números enteros no cuántico. Muchas áreas de la matemática y la ciencia de la computación están involucradas en este problema, inicialmente la teoría algebraica de números y, más recientemente, la computación cuántica.

Adicionalmente, ya existen algoritmos cuánticos para resolver estos problemas y descifrar comunicaciones digitales, como el Algoritmo de Shor, mencionado anteriormente, que solo puede ejecutarse en un ordenador cuántico. Este algoritmo es capaz de analizar y factorizar números enteros de cualquier tamaño. Por ejemplo, Gidney y Ekera indican que es posible factorizar un entero de 2048 bits en solo 8 horas, utilizando un ordenador con 20 millones de qubits. Con la tecnología actual, se necesitarían miles de años.

De esta manera, la computación cuántica tendrá muchas aplicaciones en el análisis de grandes cantidades de datos. Sin embargo, esta nueva tecnología no solo acelera la computación convencional, sino que también ofrece una mayor capacidad de procesamiento para ciertos tipos de problemas, además de la factorización de números muy grandes, como: secuenciación de ADN, inteligencia artificial y predicción del tiempo, entre otras áreas.

La transmisión segura de datos a través de la comunicación cuántica y la computación cuántica aplicada a la cibernética son de fundamental importancia. En términos de seguridad y defensa nacional, la computación cuántica será crucial, especialmente cuando se aplique a la cibernética, ya que la mayor parte de la infraestructura digital planetaria y casi todas las actividades realizadas en línea, como videoconferencias, envío de correos electrónicos y acceso remoto a cuentas bancarias, se basan en la criptografía realizada mediante protocolos que se aprovechan de la incapacidad de los recursos computacionales existentes para resolver la factorización de grandes números enteros.

Aunque los ordenadores cuánticos no tienen el poder de procesamiento para descifrar la mayoría de los métodos de criptografía, se deben encontrar maneras de protegerse contra esta amenaza, ya que los avances en la capacidad de estos ordenadores han sido significativos y, dado que las inversiones en esta área de investigación científica y desarrollo tecnológico están aumentando, la tendencia es que el ritmo de este aumento no se desacelere. Como se mencionó antes, se estima que un ordenador cuántico necesitaría tener alrededor de 20 millones de qubits para romper la criptografía RSA actual, utilizada para enviar datos confidenciales por Internet. Teniendo en cuenta que el mayor ordenador cuántico actualmente tiene 5000 qubits (D-Wave), se puede afirmar que aún falta mucho tiempo para romper esta criptografía.

En síntesis, a pesar de que aún no existen ordenadores cuánticos

comerciales para el público en general (solo dispositivos con fines educativos con un bajo número de qubits), los desarrollos en esta área ya se encuentran en una fase intermedia de madurez tecnológica. Con la perspectiva del desarrollo de ordenadores cuánticos comerciales, es factible imaginar que la información cifrada de los sistemas de comunicaciones en uso está siendo almacenada para ser utilizada en la descifrado cuando la nueva tecnología esté disponible.

De hecho, la computación cuántica es una amenaza urgente para la seguridad cibernética de la sociedad en general y de los sistemas empleados en el área de Seguridad y Defensa nacional, en particular. Para combatirla, se debe actualizar completamente toda la infraestructura digital. En este sentido, merecen destacarse algunas aproximaciones que se discutirán a continuación.

Una posibilidad para proteger la información actual contra los ordenadores del futuro es implementar lo que se conoce como criptografía post-cuántica (en inglés, Post-Quantum Cryptography – PQC). A pesar del nombre, se trata de nuevos algoritmos criptográficos clásicos (es decir, no son cuánticos), cuya solución por ordenadores cuánticos sería tan demorada como la de los algoritmos clásicos actuales.

El organismo de EE.UU. equivalente al INMETRO brasileño, el NIST (Instituto Nacional de Estándares y Tecnología), realizó una competencia/consulta internacional, en la que seleccionó tres algoritmos PQC para su estandarización y adopción global. El proceso comenzó en 2016 y, en agosto de 2023, se solicitaron comentarios públicos sobre los tres finalistas. El período de comentarios finalizó en noviembre de 2023 y la decisión final del NIST se tomó en agosto de este año. Uno de los objetivos del NIST es que los algoritmos seleccionados puedan interoperar con los protocolos y redes de comunicaciones existentes. Con los algoritmos estandarizados, se espera que el IETF (Internet Engineering Task Force), responsable del desarrollo y promoción de los estándares de Internet, los incorpore en nuevas versiones de protocolos como IPSec (siglas en inglés de IP Security protocol) y TLS (Transport Layer Security), ya en 2025.

Una opción sería esperar que la comunicación cuántica, a través de criptografía cuántica, teletransporte cuántico u otra implementación más moderna, madure hasta el punto de utilizar este tipo de comunicación para protegerse de los ataques de descifrado realizados por ordenadores cuánticos. La implementación más conocida de la criptografía cuántica son los protocolos QKD.

Invertir en la comunicación cuántica (QKD o teletransporte cuántico), promoviendo su madurez con la expectativa de que ofrezca resistencia a la amenaza cuántica, es una aproximación que están adoptando varios grupos de investigación brasileños, como las iniciativas promovidas por el IME y las universidades del proyecto RRQ. Los formuladores de políticas públicas y líderes de todas las esferas deben estar atentos y preparados para la necesidad de actualizaciones en el área de seguridad cibernética.

(d) Carrera mundial por el dominio de las Tecnologías Cuánticas

Las Tecnologías Cuánticas son transversales y tienen un amplio espectro de aplicaciones en Seguridad y Defensa nacional, siendo fundamentales para el desarrollo de nuevas capacidades militares esenciales para la Guerra del Futuro.

Los avances en las áreas asociadas con las Tecnologías Cuánticas están siendo sorprendentes, particularmente debido a los grandes intereses gubernamentales y privados que movilizan cifras extraordinarias de recursos financieros para fomentar la investigación básica, investigación aplicada y los desarrollos, así como para formar recursos humanos altamente calificados para explorar todas las facetas aún no descubiertas de las tecnologías cuánticas.

La Figura 12 muestra las inversiones realizadas en el mundo en 2022 que sumaron aproximadamente 30 mil millones de dólares (aproximadamente 160 mil millones de R$). En 2023, esta cantidad superó los 38 mil millones de USD (alrededor de 228 mil millones de R$) y se prevé que en 2040 superará los 106 mil millones de USD, más de medio billón de reales. China aparece como el mayor inversionista en el área (USD 15 mil millones). Brasil aparece con tímidos 12 millones de USD en inversiones en 2023.

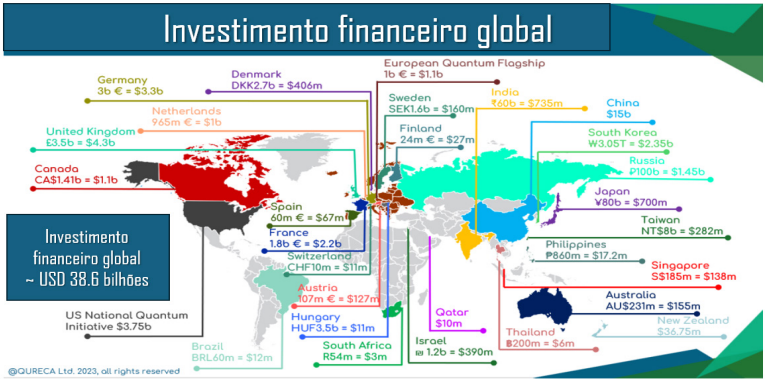


Figura 12: Inversiones realizadas en el mundo en 2023.

Además de la cuestión financiera, también se debe considerar la infraestructura nacional para el almacenamiento y tratamiento de los datos. Lo que comúnmente se conoce como la "nube" no son más que servidores distribuidos en enormes centros de datos, responsables del almacenamiento y procesamiento de los sistemas en Internet. Se trata de una cuestión de soberanía de datos: los países que no tienen soberanía sobre su infraestructura y bases de datos físicas locales corren el riesgo de que sus datos sean utilizados por otros países para el desarrollo de tecnologías cuánticas. Además, las tecnologías cuánticas, particularmente la computación y la comunicación cuántica, también necesitarán centros de datos preparados para recibir los hardware cuánticos.

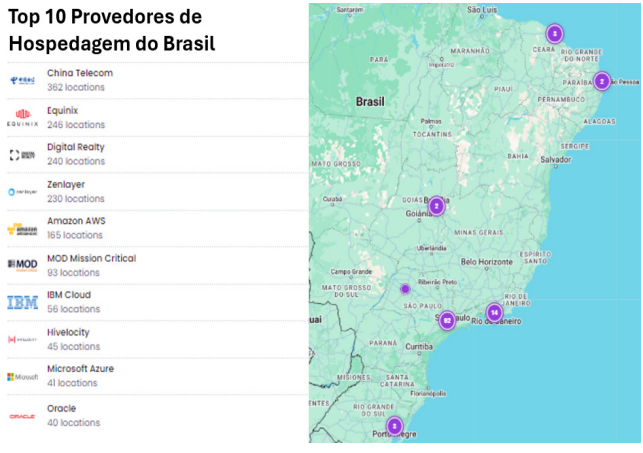


Figura 13: Distribución de los principales proveedores de alojamiento en Brasil.

Brasil cuenta con una red de datacenters aún pequeña, mal distribuida y controlada por grandes corporaciones extranjeras, como se puede ver en la Figura 13. Hay 117 datacenters en el territorio nacional, distribuidos solo en 6 estados y controlados por 26 proveedores, la mayoría de ellos extranjeros. Son estos datacenters los que almacenan la información principal de los sistemas brasileños. Por lo tanto, se trata de una cuestión de soberanía que el software y el hardware cuántico no deban ser hospedados en lugares controlados por extranjeros.

REFLEJOS DE LAS TECNOLOGÍAS CUÁNTICAS Y LA 4ª REVOLUCIÓN INDUSTRIAL EN LA DEFENSA NACIONAL

La cuarta revolución industrial se caracteriza por la fusión de las esferas física, digital y biológica, con tecnologías desarrolladas en estas tres esferas para un desarrollo más acelerado del sector productivo. En esta revolución, se obtiene una sinergia de avances e innovaciones disruptivas en diversos sectores de la ciencia y la tecnología, que, cuando se combinan, impactan las áreas más diversas de la sociedad, el crecimiento y el desarrollo económico, la seguridad y la soberanía nacional, las relaciones internacionales y, particularmente, la naturaleza de los conflictos y las guerras. En el marco de esta revolución, se identifican algunas tendencias que serán analizadas con mayor enfoque en este texto, como la hiperconectividad, la digitalización y la convergencia digital, así como el intercambio de información, por ejemplo, almacenada en la "nube". Estas tendencias tienen un gran impacto en la Seguridad y Defensa Cibernética, área que se verá fuertemente afectada por las Tecnologías Cuánticas.

Como consecuencia de este vertiginoso avance, hoy es posible identificar una internet móvil omnipresente y eficaz; reducción en el tamaño y el costo, y aumento en la capacidad de los sensores que surgen para monitorear los más variados fenómenos y objetos; además de robots; internet de las cosas (IoT), internet de las cosas en el campo de batalla (IoBT), ciudades inteligentes, vehículos autónomos, manufactura aditiva, tecnologías portátiles, enjambres de drones, armas inteligentes, entre muchas otras. Frente a la inmensidad de tecnologías que permea esta revolución, aquí se centra en las discusiones e interdependencias entre la IA, la Cibernética y las Tecnologías Cuánticas, así como algunas posibles

tendencias derivadas del uso conjunto de estas tecnologías en el área de Defensa.

A pesar de que sus bases teóricas y las primeras pruebas del concepto surgieron en la década de 1950, la IA ha proporcionado un volumen cada vez mayor de innovaciones importantes en los últimos años, gracias al fácil acceso a grandes cantidades de datos, lo que es necesario para que los algoritmos "inteligentes" puedan converger y aprender del entorno; al aumento exponencial del poder de procesamiento (Ley de Moore) y la capacidad de almacenamiento, esenciales para permitir la ejecución de algoritmos de IA en tiempo real; a los avances en el desarrollo de algoritmos de búsqueda y técnicas de aprendizaje profundo; a la disponibilidad de sensores que recogen grandes cantidades de datos en tiempo real; y a los avances en actuadores, en muchos casos indispensables para realizar acciones originadas en dispositivos dotados de IA. A medida que las nuevas tecnologías cuánticas se vuelvan viables para ser integradas, la IA podrá ser impulsada aún más, y podrá ocurrir un salto extraordinario en el desempeño de estos dispositivos y sistemas, como vehículos autónomos, enjambres de drones y robótica.

Desde el punto de vista de la industria de defensa, destacan los usos de IA en Cibernética, Redes de Sensores Inalámbricos, Simulación, Detección de Objetos, Vehículos Aéreos No Tripulados (VANT), Sistemas de Comando y Control y Sistemas Mecatrónicos. Así, la selección, detección y compromiso de objetivos, así como el uso automatizado de enjambres de drones, son algunas de las posibilidades del uso de la IA en la Guerra del Futuro. La IA es una tecnología que ya existía anteriormente en un formato diferente, creada para obtener mayor eficiencia en tareas específicas y no generativas. Más recientemente, la inteligencia artificial, teniendo como principal representante en la población en general el ChatGPT (o GPT-3, Generative Pre-Trained Transformer) de la empresa Open IA, ha dado indicios de la revolución científica, tecnológica y social que está experimentando el área de IA.

El GPT-4 utilizará 100 billones de parámetros, mucho más que los 175 mil millones de parámetros de la versión GPT-3. Algunos científicos consideran que la nueva versión, el GPT-5, podría convertirse en una Inteligencia Artificial General (IAG). Para que esto sea posible, aún debemos esperar los próximos resultados. Las versiones ChatGPT-3.5 y 4 son conocidas por degradarse cuando se usan de forma extensa por varios usuarios, un fenómeno llamado desviación conductual o "model

drift". Superando tales obstáculos, la IA, asociada con la capacidad de procesamiento y almacenamiento de las Tecnologías Cuánticas, deberá presentar capacidades mucho mayores que las conocidas actualmente.

La electrónica embarcada y los componentes basados en software están comenzando a desempeñar un papel importante en artefactos y vectores aéreos, marítimos y terrestres. El advenimiento de redes cognitivas, la computación en la nube y los avances en las comunicaciones digitales a través de canales inalámbricos están aumentando la conectividad. Las tecnologías clave que sustentan estas cuestiones permiten que las Fuerzas Armadas desarrollen principios de guerra cibernética, empleen sistemas complejos de comando y control, y perciban situaciones de campo de batalla de manera intuitiva y con detalles sin precedentes. La seguridad, respaldada por protocolos basados en tecnologías cuánticas, estará a la vanguardia del diseño y la operación de sistemas de guerra inteligentes y sus redes de apoyo. El progreso es grande para quienes dominen las tecnologías críticas, pero representará un gran retroceso y grandes amenazas para los países con baja capacidad tecnológica acumulada en áreas clave.

En el contexto de la 4ª Revolución Industrial, surge la Guerra Cibernética, cuya vulnerabilidad de seguridad aumenta con la dependencia de la tecnología, sobre todo con el advenimiento de las tecnologías cuánticas. La primera definición formal de Guerra Cibernética se atribuye frecuentemente a los investigadores John Arquilla y David Ronfeldt, en un informe publicado en 1993 por el think tank RAND Corporation. Ellos definieron la Guerra Cibernética como: "Conducir y prepararse para conducir operaciones militares de acuerdo con principios relacionados con la información. Esto significa ataques cuyo objetivo es desactivar, interrumpir o destruir los sistemas de información y comunicación del adversario, mientras se protege los propios sistemas." Con la 4ª Revolución Industrial, las infraestructuras críticas se vuelven conectadas en red y al ciberespacio, haciendo que los impactos de este tipo de guerra sean aún mayores. Las Tecnologías Cuánticas impulsarán este impacto.

Entre los meses de junio y octubre de 1999, Jonathan, un adolescente estadounidense de apenas 15 años, hackeó la NASA y el Pentágono, además de otros objetivos más pequeños. Se convirtió en la primera persona en el mundo en entrar en el sistema de la Defense Threat Reduction Agency (DTRA), una división del DoD (Department of Defense) encargada de analizar posibles amenazas para los Estados Unidos. La

misma hazaña respecto al Pentágono fue alcanzada por otros hackers, como Gary McKinnon, acusado de haber invadido, entre febrero de 2001 y marzo de 2002, los ordenadores de la NASA, el Pentágono, el Ejército (USARMY), la Fuerza Aérea (USAF) y la Marina (USNAVY) de los Estados Unidos. Los fiscales estadounidenses acusaron a McKinnon de haber apagado completamente una red de más de 2 mil computadoras, durante 24 horas. Los ataques de hackers rusos han sido noticia desde las últimas elecciones presidenciales de Estados Unidos hasta más recientemente, durante la Guerra Rusia-Ucrania.

En 2016, una simple foto (Figura 14), compartida por Mark Zuckerberg para celebrar los 500 millones de usuarios de Instagram, volvió a poner el tema de los hackers en discusión. En la imagen, se puede ver que el creador de Facebook cubrió con cinta adhesiva la webcam y el micrófono de su computadora portátil. Definitivamente, nadie en el mundo está libre de los hackers.

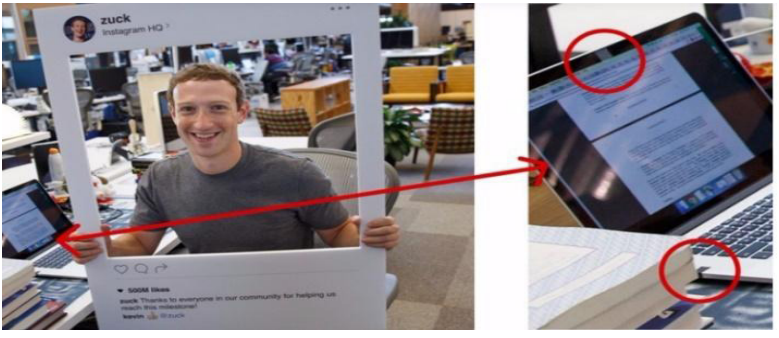


Figura 14: Foto compartida por Mark Zuckerberg para celebrar los 500 millones de usuarios de Instagram volvió a poner el tema de los hackers en discusión.

En 2018, China fue acusada de invadir los sistemas de la Marina de EE. UU. Según la información obtenida por el periódico The Washington Post a partir de funcionarios no identificados de las Fuerzas Armadas de EE. UU., hackers chinos habrían invadido los sistemas de una empresa subcontratada que presta servicios a las Fuerzas Armadas estadounidenses y accedido a alrededor de 614 GB de datos confidenciales.

A mediados de junio de 2023, la Marina de EE. UU. fue nuevamente invadida por hackers chinos. Microsoft emitió una alerta, al igual que las agencias de inteligencia, incluyendo la Agencia de Seguridad Nacional,

la Agencia de Ciberseguridad e Infraestructura, y las agencias de ciberseguridad de otras cuatro naciones. Las alertas informaron a empresas públicas y privadas de que un sofisticado grupo de hackers, respaldado por el gobierno chino, había explotado con éxito una vulnerabilidad en un popular paquete de seguridad cibernética. Con el Volt Typhoon, este supuesto grupo chino afectó la infraestructura crítica cibernética en varios sectores. Según los informes, los hackers chinos se centraron en las comunicaciones y los sectores marítimos en la isla de Guam, en el Pacífico, que alberga una importante base militar de EE. UU.

Recientemente, el periódico The New York Times informó que Estados Unidos trabaja para identificar y eliminar un código malicioso que, según el artículo, fue instalado por China en el corazón de las redes que controlan la infraestructura crítica del Ejército estadounidense, con la posibilidad de que se active a distancia en caso de un conflicto armado (por ejemplo, en una guerra entre China y Taiwán) e interrumpa las redes de electricidad, agua potable y comunicación que abastecen las bases militares estadounidenses, dificultando el despliegue de estas tropas. Esto muestra las posibles consecuencias desastrosas que una defensa cibernética ineficaz podría causar a la seguridad de cualquier país.

Con las tendencias derivadas de la cuarta revolución tecnológica y sus consecuencias, como la digitalización e hiperconectividad, incluso de los sistemas y materiales militares, la superficie de ataque cibernético aumentará aún más. Los ciberataques y el espionaje digital se intensificarán, y sus consecuencias se volverán más graves.

El estudio de la cuarta revolución industrial y la guerra cibernética se ha vuelto central para el desarrollo del arte y el pensamiento militar. En esta nueva era, la dependencia de la tecnología será extremadamente grave para un país debido al aumento de las vulnerabilidades cibernéticas. Las evidencias sugieren que las tecnologías cuánticas serán fundamentales para el equilibrio entre una mayor protección o una mayor vulnerabilidad cibernética, ya que los avances tecnológicos impulsan tanto innovaciones para la defensa como para la violación de la seguridad de los sistemas de comunicación de datos. Se puede inferir que un sistema de protección basado en el uso de comunicación cuántica, computación cuántica, criptografía, así como el uso de dispositivos (sensores, detectores y actuadores) basados en estas tecnologías será eficiente. De esta forma, alcanzar la llamada supremacía cuántica es un objetivo esencial para un país que aspire a desempeñar un papel relevante en el concierto de las

naciones, así como promover por sus propios medios la soberanía nacional.

Al analizarse los diferentes teatros de operaciones de los últimos conflictos o crisis, como el que ocurre entre China y Taiwán, observamos fuertes señales de un sorprendente avance tecnológico. Un ejemplo de ello es el desarrollo del dron ruso llamado Joker, que puede permanecer en reposo (o en modo de hibernación) durante semanas.

Diseñado para esconderse de contramedidas electrónicas, el dron podría prepararse para el ataque horas, días o semanas antes de que su operador lo despierte para desencadenar la misión. Los avances no se detienen, lo que sugiere el uso intensivo de las Tecnologías Cuánticas por parte de las grandes potencias en el mediano plazo, y en un futuro no muy lejano, la guerra podría ser dominada por el uso de las tecnologías cuánticas, configurando lo que se denomina Quantum Warfare (Figura 01) o Guerra Cuántica.

Las discusiones presentadas en la Sección 3 traen a colación la famosa frase pronunciada en 1915 por el almirante británico John Fisher. Durante la Primera Guerra Mundial (1914-1918), él declaró que la guerra la ganarán las invenciones. Las características de los conflictos actuales y las tendencias de evolución en el campo científico-tecnológico, especialmente en el área de las tecnologías cuánticas, sugieren que esta afirmación es profética.

Pero a pesar de los avances tecnológicos, la llamada Guerra del Futuro aún no ha llegado, ya que estos nuevos conceptos todavía están siendo incorporados a las diferentes fuerzas. Las máquinas con IA de última generación deberían ser, en breve, una realidad. Ya hay varios estados de EE. UU. que están comenzando a utilizar robots de Boston Dynamics para el patrullaje preventivo de las ciudades (entre ellas, Los Ángeles, Nueva York y San Francisco).

.

Figura 15: Arma anti-blindagem de ombro, denominada Javelin, dispara um míssil autoguiado contra o seu alvo.

A pesar de las tácticas de emboscada y del hecho de que Rusia no está utilizando sus tanques más modernos, la actual guerra entre Ucrania y Rusia ha demostrado que la tecnología de los lanzadores de misiles Javelin (Figura 15) puede representar un riesgo, en términos de poder de fuego, para la flota de vehículos blindados rusos. Esta arma anti-blindaje de hombro fue desarrollada y fabricada para el Marine Corps/US Army por Lockheed Martin (Florida) y Raytheon (Arizona), pero aún no incorpora conceptos relacionados con la tecnología cuántica, ya que aún no son aplicables. Cuando esto suceda, podrían ocurrir avances extraordinarios en áreas como la inteligencia artificial, robótica, cibernética, comunicaciones y sistemas de mando y control, con innumerables consecuencias en la capacidad de defensa y poder de combate de las fuerzas.

Ante esta efervescencia de innovaciones tecnológicas, en 2021 se consolidó un cambio fundamental en la política de defensa de muchos países considerados potencias militares, caracterizado por el crecimiento del presupuesto para la tecnología digital, inteligencia artificial, cibernética y tecnologías cuánticas, y por la disminución de los fondos tanto para equipos convencionales como para el mantenimiento de grandes tropas.

CONSIDERACIONES FINALES

En este artículo, se abordó, de manera general, la influencia de las tecnologías derivadas de la Segunda Revolución Cuántica, especialmente en las áreas de Seguridad y Defensa nacional. Las evidencias presentadas aquí sugieren que la adopción de un programa estratégico del

Ejército Brasileño en esta área es una cuestión de soberanía. Los países desarrollados o que desean adquirir prominencia en el concierto de las naciones invierten fuertemente en I+D para obtener diversas aplicaciones militares en Tecnologías Cuánticas. La computación, la comunicación, el sensoreo y la criptografía cuántica representan la única manera de disponer de comunicación segura a prueba de hackers, conciencia situacional y el desarrollo eficiente de capacidades militares centrales para la Guerra del Futuro.

Dado el enorme impacto de las tecnologías cuánticas en el área de cibernética, y dada la fuerte dependencia actual del mundo con respecto a las computadoras, este estudio abordó muchos aspectos relacionados con la Guerra Cibernética. En un conflicto bélico, financiero, etc., es común que las infraestructuras críticas sean atacadas al inicio para desestabilizar a una nación. Actualmente, todas las infraestructuras críticas dependen de una red computacional sofisticada que se convierte cada vez más en un objetivo para los agresores. En todos los casos, se vislumbra que la mejor estructura de Seguridad y Defensa Cibernética utilizará las Tecnologías Cuánticas.

La posibilidad de obtener información indebidamente dentro de una red de comunicación, en tiempos extremadamente cortos, con el algoritmo de Shor, por ejemplo, es preocupante. Así, el conjunto de tecnologías cuánticas aplicables a la cibernética, junto con el área de dispositivos (sensores, biosensores y detectores) cuánticos, son esenciales para que las Fuerzas Armadas puedan cumplir sus misiones constitucionales. En el futuro, la asociación de estas tecnologías con otras, como la IA, será determinante en robótica, sistemas autónomos, VANTS, misilística y fundamentará la llamada Guerra Cuántica.

Dada esta gran importancia estratégica y los objetivos marcadamente diferentes de los tres principales actores: el medio académico, las empresas y el gobierno, especialmente las Fuerzas Armadas, es seguro afirmar que el desarrollo e implementación de las Tecnologías Cuánticas debe ser gestionado y liderado por las Fuerzas Armadas, en particular por el Ejército Brasileño, enfocado en el área de cibernética. Esto, porque corresponde a las otras fuerzas encargarse de las otras dos grandes áreas estratégicas: la Nuclear y la Aeroespacial, tal como se establece en la Estrategia Nacional de Defensa.

Las Tecnologías Cuánticas enfrentan actualmente varios desafíos tecnológicos, tales como: la frecuente necesidad de operar a temperaturas

extremadamente bajas; decoherencia; ruido cuántico; escalabilidad; materiales adecuados; y costos aún elevados. Aunque este hecho puede ser visto como un problema, tales desafíos también representan una oportunidad, pues esto significa que la tecnología aún no está lista y existe espacio para un desarrollo nacional. Es importante destacar que invertir en esta tecnología implica competir con otras políticas públicas brasileñas.

Sin embargo, debido al gran esfuerzo global en términos de inversiones en Tecnologías Cuánticas, Brasil y, particularmente, sus Fuerzas Armadas no pueden mantenerse indiferentes. Las inversiones mundiales indican básicamente una cosa: quien no domine las Tecnologías Cuánticas pagará un alto precio estratégico en Seguridad y Defensa Nacional, además de en crecimiento y desarrollo económico y tecnológico. Integrado al Programa de Defensa Cibernética en la Defensa Nacional (PDCDN), el Ejército Brasileño desarrolla su Programa Estratégico de Defensa Cibernética, que tiene como finalidad coordinar e integrar los proyectos y procesos del Sector Cibernético, así como desarrollar las capacidades cibernéticas de las Fuerzas Armadas, a través de integración, coordinación y acción conjunta. El PDCDN ha buscado, desde 2023, proporcionar recursos para el desarrollo de Tecnologías Cuánticas nacionales.

De esta manera, Brasil no puede ignorar la importancia estratégica del desarrollo nacional de estas tecnologías y simplemente optar por su importación, tanto de productos (sistemas de comunicación, internet y criptografía cuántica y sensores cuánticos) como de servicios (computadoras cuánticas). Es inconcebible que datos estratégicos y confidenciales sobre las operaciones de nuestras Fuerzas Armadas sean analizados por computadoras cuánticas extranjeras como el Sycamore (de Google) o el Osprey (de IBM) debido a la falta de equipos nacionales.

No hay muchas dudas sobre la necesidad urgente y esencial del desarrollo local de las Tecnologías Cuánticas de aplicación en seguridad y defensa nacional. Sin embargo, debido a los enormes desafíos científicos y tecnológicos y la dualidad de las tecnologías a desarrollar, con fuerte impacto en todas las Expresiones del Poder Nacional, para alcanzar el resultado deseado en estas tecnologías disruptivas, debe promoverse un esfuerzo nacional en la asignación de los recursos financieros necesarios para lograr autonomía en un área estratégica para el país.

Los políticos, estrategas y decisores que defienden los valores de la libertad, democracia y soberanía reconocen que su preservación depende de una vigilancia constante, es decir, de un sistema de Defensa

Nacional que pueda repeler amenazas actuales y futuras. Mantener un sistema de vigilancia permanente es el precio a pagar por algo tan valioso. Como resumió Rui Barbosa: "Un ejército puede pasar 100 años sin uso, pero ni un minuto sin preparación". Este modo de pensar da las bases para el sentido de autopreservación y cohesión nacional que orientará las inversiones en el área de Defensa.

Aunque diversas áreas del Poder Nacional pueden ser movilizadas para actuar por la soberanía de una nación, el Estado debe coordinar, recolectar e integrar los Sistemas y Materiales de Empleo Militar (SMEM) para fortalecer las capacidades de su sistema militar. Esta robustez requiere necesariamente autonomía tecnológica. En términos de tecnología de Defensa, nada es más moderno y fundamental que las Tecnologías Cuánticas. Tienen el potencial de afectar casi todos los aspectos del entorno militar, desde aquellos que poseen poco contenido científico-tecnológico hasta los más complejos.

Apoyándose en innovaciones tecnológicas autóctonas de alto valor agregado, esenciales para la supervivencia del Estado y la concreción de los llamados Objetivos Nacionales Permanentes, en general, el sector de la Defensa es el motor propulsor del desarrollo científico y tecnológico y eleva el mercado multimillonario de las empresas que componen la Base Industrial de Defensa (BID). Indispensables para incentivar proyectos innovadores, especialmente aquellos directamente relacionados con la Defensa Nacional, los mecanismos adoptados por el Estado para apoyar la BID disponen de pocos estudios que caractericen los factores relacionados con su origen o desarrollo. Sin embargo, se sabe que los principales actores en este ámbito, como Estados Unidos, la Unión Europea, Gran Bretaña y Rusia, ganaron las grandes guerras del siglo XX gracias a una próspera industria de Defensa y un apoyo financiero constante e importante en las áreas de educación, ciencia y tecnología, demostrando así la importancia de este trío para sus pueblos en la resolución de conflictos.

Es esencial definir los objetivos a corto, medio y largo plazo; coordinar y evaluar los avances en la comunidad académica y de ICTs, así como contribuir con investigaciones en el sector, a través de sus ICTs en colaboración con la comunidad académica, empresas y otros sectores gubernamentales. Esto incluye no solo asociaciones con grandes empresas tecnológicas, sino sobre todo con startups, universidades e institutos de investigación, pues son esenciales para la innovación en este tipo de tecnología. Sin embargo, dado que el contenido es sensible y

de vital importancia para la Seguridad y Defensa del país, este proceso debe involucrar una participación significativa de las Fuerzas Armadas, especialmente del Ejército Brasileño, en particular, de sus organizaciones de enseñanza, investigación, desarrollo e innovación. Una iniciativa en este sentido fue recientemente aprobada por la CAPES (PRO-DEFESA-V) y, con la coordinación del IME, que involucra aproximadamente 100 investigadores de 43 instituciones civiles y militares y 23 programas de posgrado.

Para que las Fuerzas Armadas puedan realmente disfrutar de los beneficios de estas nuevas Tecnologías Cuánticas, es fundamental que participen activamente en esta área y proporcionen tanto las bases del desarrollo como la adopción de aplicaciones de los posibles usos en el ámbito militar. Un fuerte involucramiento en el ecosistema cuántico mejorará la comprensión de las Fuerzas Armadas sobre los riesgos potenciales asociados con estas nuevas tecnologías, especialmente en el área de cibernética. Tal riesgo queda evidente cuando se tiene en cuenta la importancia del desarrollo de la internet cuántica, basada en la comunicación cuántica.

Es difícil imaginar una frase más actual y relevante que la dicha en 1915 por el Almirante británico John Fisher cuando afirmó que "la Guerra será ganada por las invenciones". Analizando, a la luz del texto anterior, lo dicho por el 3er Visconde Palmerston – "No tenemos aliados eternos, ni enemigos perpetuos. Nuestros intereses son eternos y perpetuos" – queda cristalina la necesidad urgente de desarrollar nuestras propias Tecnologías Cuánticas relacionadas con Seguridad y Defensa. Las tecnologías cuánticas son esenciales para el crecimiento económico, el desarrollo y la soberanía de un país. Al perder la oportunidad de explorar adecuadamente algunas revoluciones tecnológicas, como la microelectrónica y la nanotecnología, Brasil sufrió pérdidas incalculables e irreversibles. Los países que no dominen las Tecnologías Cuánticas podrían sufrir una verdadera catástrofe, en términos socioeconómicos y de soberanía.

En 2025, el mundo celebra el Año Internacional de la Ciencia y Tecnología Cuántica, una iniciativa de la ONU. Brasil tiene todas las condiciones para acelerar el paso y aprovechar los recursos políticos y financieros que deberían surgir de esta celebración. En Brasil, el Ministerio de Ciencia, Tecnología e Innovación (MCTI) también creó un grupo de trabajo para crear propuestas en el área de Cuántica. Se espera que esta iniciativa dé inicio a la creación de la Estrategia Brasileña de

Cuántica, siguiendo los mismos moldes de la EBIA (Estratégia Brasileira de Inteligência Artificial). Es decir, el ámbito político nacional ya se está convenciendo de la importancia del tema.

O desarrollamos internamente las Tecnologías Cuánticas necesarias o nuestros sectores de Seguridad y Defensa nacional se volverán obsoletos en poco tiempo, con consecuencias desastrosas e irreversibles. Nadie hará nuestra tarea por nosotros.

REFERENCIAS

ADVANTAGE: The most connected and powerful quantum computer built for business. **D-Wave Systems**. Disponível em: https://www.dwavesys.com/solutions-and-products/systems/. Acesso em: jun. 2024.

ALVAREZ, Raúl. Jonathan James, el joven que con sólo 15 años hackeó y puso de cabeza a la NASA y al Pentágono. **Xataka**, 18 fev. 2020. Disponível em: https://www.xataka.com/historia-tecnologica/joven-que-solo-15-anos-hackeo-puso-c abeza-a-nasa-al-pentagono. Acesso em: jun. 2024.

ARAÚJO-MOREIRA, Fernando M. et al. Tecnologias quânticas: a inovação disruptiva como diferencial estratégico para a Defesa Nacional. **Seven Editora**, [S. l.], 2023. Disponível em: https://sevenpublicacoes.com.br/editora/article/view/1561. Acesso em: jun. 2024. DOI: 10.56238/tecavanaborda-042.

ARAUJO-MOREIRA, F. M.; Supremacia quântica e Defesa nacional: a nova realidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 245–247, 2023. ISBN 978-65-87080-44-4.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming!. **RAND Corporation**, 1993. Disponível em: https://www.rand.org/pubs/reprints/RP223.html. Acesso em: nov. 2024.

BARONE, A.; PATERNÒ, G. **Physics and applications of the josephson effect.** New York: John Wiley & Sons, 1982. DOI:10.1002/352760278X.

BARZANJEH, S. et al. Microwave quantum illumination using a digital receiver. **Science Advances**, v. 6, n. 19, p. 1-9, 8 mai. 2020. DOI:10.1126/sciadv.abb0451.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. **International Conference on Computers, Systems & Signal Processing**, Bangalore, vol. 1, p. 175–179, 1984. Disponível em: https://www.karlin.mff.cuni.cz/~holub/soubory/BB84original.pdf. Acesso em: jun. 2024.

BERENDSEN, René G. **The Weaponization of Quantum Mechanics: Quantum Technology in Future Warfare**. 2019. 60f. School of Advanced Military Studies, US Army Command and General Staff College. Dissertação de Mestrado, mai. 2019. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1083173.pdf. Acesso em: jun. 2024.

BOTHNER, Daniel; RODRIGUES, Ines C.; FRANSE, Jasper; STEELE, Gary. TN2953-P The Josephson junction: Quantum tunnelling and interference in an electrical circuit. **NS Web**. Disponível em: https://nsweb.tn.tudelft.nl/~gsteele/SQUID_practicum/TN2513-P%20SQUID%20Prac ticum%20 Manual.html. Acesso em: jun. 2024.

BOUTIN, Chad. NIST releases first 3 finalized post-quantum encryption standards. **NIST**, 13 ago. 2024. Disponível em: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-q uantum-encryption-standards. Acesso em: outubro de 2024.

BRANDOM, Russell. Google's quantum computer just flunked its first big test. **The Verge**, 19 jun. 2014. Disponível em: https://www.theverge.com/2014/6/19/5824336/google-s-quantum-computer-just-flunk ed-its-first-big-test. Acesso em: jun. de 2024.

BRASIL. Ministério da Defesa. **IME se destaca em Programa de Ensino e Pesquisa em Defesa**. Exército Brasileiro, 26 ago. 2024. Disponível em: https://www.eb.mil.br/web/noticias/w/ime-se-destaca-no-pro-defesa-v-principal-edital -da-capes-destinado-a-area-da-defesa. Acesso em: junho de 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 8.194, de 19 de maio de 2024**. Institui grupo de trabalho com o objetivo de debater e propor as bases e diretrizes para o estabelecimento de uma Iniciativa Brasileira para Tecnologias Quânticas. Diário Oficial da União: seção 1, Brasília, DF, n. 97, p. 87, 21 mai. 2024. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mcti-n-8.194-de-19-de-maio-de-2024-56075 5075. Acesso em: out. 2024.

BRAZIL data centers locations. **Datacenters.com**, 2024. Disponível em

https://www.datacenters.com/locations/brazil. Acesso em: nov. 2024.

CHEN, Stephen. The end of stealth? New chinese radar capable of detecting 'invisible' targets 100km away. **South China Morning Post**, Beijing, 21 set. 2016. Disponível em: https://www.scmp.com/news/china/article/2021235/end-stealth-new-chinese-radar-capable-detecting-invisible-targets-100km. Acesso em: jun. 2024.

CLARKE, John. SQUIDs. **Scientific American**, v. 271, n. 2, p. 46–53, ago. 1994. DOI: 10.1038/scientificamerican0894-46.

CORREIA, Flávia. China quebra recorde de distância de comunicação direta com segurança quântica. **Olhar Digital**, 20 abr. 2022. Disponível em: https://olhardigital.com.br/2022/04/20/ciencia-e-espaco/china-quebra-recorde-de-dist ancia-de-comunicacao-direta-com-seguranca-quantica/. Acesso em: jun. 2024.

COWING, Keith. The world's first integrated quantum communication network. **SpaceRef**, 7 jan. 2021. Disponível em: https://spaceref.com/newspace-and-tech/the-worlds-first-integrated-quantum-commu nication-network/. Acesso em: jun. 2024.

CRAWFORD, Scott E. et al. Quantum sensing for energy applications: review and perspective. **Advanced Quantum Technologies**, v. 4, n. 8, ago. 2021. DOI: 10.1002/qute.202100049.

DÓLAR cotado a R$ 6,00 em novembro de 2024. **Banco Central do Brasil**, 2024. Disponível em: https://www.bcb.gov.br. Acesso em: nov. 2024

EMMERT-STREIB, Frank. Is ChatGPT the way toward artificial general intelligence. **Discover Artificial Intelligence**, v. 4, n. 32, 2024. DOI: 10.1007/s44163-024-00126-3.

FACEBOOK: esta simple foto ha revelado que Mark Zuckerberg es muy paranoico. **RPP Noticias**, 21 jun. 2016. Disponível em: https://rpp.pe/virales/facebook/facebook-esta-simple-foto-ha-revelado-que-mark-zuc kerberg-es-muy-paranoico-noticia-973116. Acesso em: jun. 2024.

FRANÇA JUNIOR, J. A.; GALDINO, J. F. Gestão de sistemas de material de emprego militar: o papel dos níveis de prontidão tecnológica. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 13, n. 47, p. 155-176, 23 jul. 2019.

FANCHINI, Felipe. Brasil precisa acelerar o passo para se beneficiar da segunda onda de inovação quântica. **The Conversation**, 23 jul. 2024. Disponível em: https://theconversation.com/brasil-precisa-acelerar-o-passo-para-se-beneficiar-da-se gunda-onda-de-inovacao-quantica-226799. Acesso em: out. 2024.

GALANTE, Alexandre. Radar quântico – fim do stealth?. **Poder Aéreo**, 7 mai. 2018. Disponível em: https://www.aereo.jor.br/2018/05/07/radar-quantico-fim-do-stealth/. Acesso em: jun. 2024.

GALDINO, J. F.; SCHONS, D. L. Maquiavel e a Importância do Poder Militar Nacional. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 56, p. 353-368, 2022.

GALDINO, J. F. Base industrial de Defesa: ambivalência e sustentabilidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 397–400, 2023. ISBN 978-65-87080-44-4.

GALDINO, J. F. Lições sobre os desafios enfrentados pela indústria de Defesa do Brasil no período de 1950 a 1990. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 393–396, 2023. ISBN 978-65-87080-44-4.

GARDNER, Frank. As armas de guerra do futuro que já são realidade. **BBC News Brasil**, 7 jan. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-59904239. Acesso em: jun. 2024.

GIDNEY, Craig; EKERA, Martin. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **Quantum**, v. 5, p. 433, 2021. Disponível em: https://quantum-journal.org/papers/q-2021-04-15-433/. Acesso em: out. 2024. DOI: 10.22331/q-2021-04-15-433.

GIRARDI, Romullo; FRANÇA JUNIOR, J. A.; GALDINO, J. F. Criticidade tecnológica na área de defesa em países em desenvolvimento: conceitos e critérios. **Revista de Gestão e Secretariado**, v. 15, n. 4, p. 3618, 2024. ISSN: 2178-9010.

GIRARDI, R.; FRANÇA JUNIOR, J. A.; FERREIRA GALDINO, J. A customização de processos de avaliação de prontidão tecnológica baseados na escala TRL: desenvolvimento de uma metodologia para o Exército Brasileiro. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 57, p. 491-527, 28 set. 2022.

HACKERS patrocinados pelo estado chinês se infiltraram na infraestrutura naval dos EUA, diz secretário da Marinha. **Poder Naval**, 26 mai. 2023. Disponível em: https://www.naval.com.br/blog/2023/05/26/hackers-patrocinados-pelo-estado-chines se-infiltraram-na-infraestrutura-naval-dos-eua-diz-secretario-da-marinha/. Acesso em: jun. 2024.

HACKER que invadiu Pentágono perde novo recurso para evitar extradição. **Globo.com**, 31 jul. 2009. Disponível em: https://g1.globo.com/Noticias/Tecnologia/0,,MUL1249916-6174,00.html. Acesso em: jun. 2024.

IYER, Kaanita. Autoridades dos EUA procuram software chinês invasor que pode afetar operações militares. **CNN Brasil**, 30 jul. 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/autoridades-dos-eua-procuram-software chines-invasor-que-pode-afetar-operacoes-militares/. Acesso em: jun. 2024.

JAVELIN Weapon System. **Lockheed Martin**. Disponível em: https://www.lockheedmartin.com/en-us/products/javelin.html. Acesso em: jun. 2024.

KRATIUK, Anton. Russian stealth drone S-70 uses high-tech components of Western manufacture: ukrainian experts present evidence. **Gagadget**.com, 8 nov. 2024. Disponível em: https://gagadget.com/en/528077-russian-stealth-drone-s-70-uses-high-tech-components-of-western-manufacture-ukrainian-experts-present-evidence/. Acesso em: nov. 2024.

KRELINA, M. Quantum technology for military applications. **EPJ Quantum** Technology. v. 8, n. 24, 2021. DOI: 10.1140/epjqt/s40507-021-00113-y.

LANÇADA a pedra fundamental da Rede Rio Quântica. **Portal Gov.br**, 11 mai. 2023. Disponível em: https://www.gov.br/cbpf/pt-br/assuntos/noticias/lancada-a-pedra-fundamental-da-red e-rio-quantica. Acesso em: jun. 2024.

LEFFER, Lauren. Yes, AI models can get worse over time. **Scientific American**, 2 ago. 2023. Disponível em: https://www.scientificamerican.com/article/yes-ai-models-can-get-worse-over-time/. Acesso em: nov. 2024.

MALIK, Mehul; MAGAÑA-LOAIZA Omar S.; BOYD, Robert W. Quantum-secured imaging. **Applied Physics Letters**, v. 101, n. 24, 10 dez. 2012. DOI: 10.1063/1.4770298.

MCFADDEN, Christopher. Russia has developed a new kind of 'sleeper' drone called the 'Joker'. **Interesting Engineering**, 26 jul. 2023. Disponível em: https://interestingengineering.com/innovation/russia-sleeper-drone-the-joker. Acesso em: jun. 2024.

MONTEIRO, Luís N. C. S. Guerras de 4a geração. **Revista Militar**, Lisboa, v. 2591, p. 1001-1014, dez. 2017. Disponível em: https://www.revistamilitar.pt/artigo/1288. Acesso em: jun. 2024.

MÜLLER, Léo. China é acusada de hackear marinha dos EUA e roubar projeto bélico. **Tecmundo**, 8 jun. 2016. Disponível em: https://www.tecmundo.com.br/seguranca/131129-china-acusada-hackear-marinha-eua-roubar-projeto-belico.htm. Acesso em: jun. 2024.

MURRAY, W.; KNOX, M. A. **Evolução da arte da guerra**: das guerras medievais aos ataques relâmpagos 1300 - 2050. Rio de Janeiro: BIBLIEx, 2022, 292 p.

NEWDICK, Thomas. Russia's S-70 hunter drone was armed when shot down by friendly fighter over Ukraine. **The Warzone**, 7 out. 2024.

Disponível em: https://www.twz.com/air/russias-s-70-hunter-drone-was-armed-when-shot-down-by-fr iendly-fighter-over-ukraine. Acesso em: nov. 2024.

O QUE é comunicação quântica?. **Mit Technology Review**, [s. l.], 1 set. 2020. Disponível em: https://mittechreview.com.br/o-que-e-comunicacao-quantica/. Acesso em: jun. 2024.

PADILHA, Luiz. YlC-8E: o primeiro radar anti-stealth do mundo. **Defesa Aérea & Naval**, 8 out. 2021. Disponível em: https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/ylc-8e-o-primeiro-radar-a nti-stealth-do-mundo. Acesso em: jun. de 2024.

PADILLA CRUZ, A. M. **Quantum Technology and its influence in Global Power Politics**. 2020. 101f. Dissertação (Mestrado Internacional em Segurança, Inteligência e Estudos Estratégicos) - Charles University. 16 set. 2020. Disponível em: https://dspace.cuni.cz/bitstream/handle/20.500.11956/177264/120370453.pdf?seque nce=1&isAllowed=y. Acesso em: nov. 2024.

PANASOVSKIY, Maksim. Chinas Tarnkappenbomber H-20 wird Atomwaffen tragen und konventionelle Einsätze fliegen. **Gagadget.com**, [s. l.], 27 out. 2023. Disponível em: https://gagadget.com/de/342722-chinas-tarnkappenbomber-h-20-wird-atomwaffen-tr agen-und-konventionelle-einsatze-fliegen/. Acesso em: jun. 2024.

PAYÃO, Felipe. China cria radar quântico que revela qualquer caça stealth no mundo. **Tecmundo**, 26 set. 2016. Disponível em: https://www.tecmundo.com.br/tecmundo-auto/109884-china-cria-radar-quantico-revela-qualquer-caca-stealth-mundo.htm. Acesso em: jun. 2024.

PICCHI, Aimee. Los Angeles approves $278,000 robot police dog despite "grave concerns". **CBS News**, 24 mai. 2023. Disponível em: https://www.cbsnews.com/news/los-angeles-robot-police-dog-approved-despite-grave-concerns/. Acesso em: jun. 2024.

PRESKILL, John. Quantum computing 40 years later. **Quantum Physics**, 19 jun. 2021. DOI: 10.48550/arXiv.2106.10522.

POST-QUANTUM Cryptography. **NIST**, 2017. Disponível em: https://www.nist.gov/pqcrypto. Acesso em: jun. 2024.

QUANTUM Manifesto - A new era of technology. **TNO**, 2016. Disponível em: https://www.tno.nl/media/7638/quantum_manifesto.pdf. Acesso em: jun. 2024.

QUANTUM RESOURCES AND CAREERS. Quantum Initiatives Worldwide 2023. **QURECA**. Disponível em: https://www.qureca.com/quantum-initiatives-worldwide/. Acesso em: out. 2024.

RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard M. A method for obtaining digital signatures and public key signatures. **ACM Digital Library**, vol. 21, n. 2, 1 fev. 1978. DOI: https://doi.org/10.1145/359340.359342.

RUSSIAN combat UAV Sukhoi S-70 Okhotnik made first flight. **Army Recognition Group**, 5 ago. 2019. Disponível em: https://www.armyrecognition.com/news/army-news/2019/russian-combat-uav-sukhoi s-70-okhotnik-made-first-flight. Acesso em: nov. de 2024.

SHOR, Peter W. Algorithms for quantum computation: discrete logarithms and factoring. **35th Annual Symposium on Foundations of Computer Science**, Santa Fé, p. 124-134, 1994. DOI: 10.1109/SFCS.1994.365700.

TECHNOLOGY Readiness Level of Quantum Computing Technology (QTRL). **Jülich Forschungszentrum**, 19 jul. 2022. Disponível em: https://www.fz-juelich.de/en/ias/jsc/about-us/structure/research-groups/qip/technolog y-readiness-level-of-quantum-computing-technology-qtrl. Acesso em: jun. 2024.

TREATY of Adrianople - Charges Against Viscount Palmerston. **UK Parliament [Hansard, House of Commons Debate]**, vol. 97, p. 66-123, 01 mar. 1848. Disponível em: https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople -charges-against. Acesso em: nov. de 2024.

VAN AMERONGEN, Michiel. Quantum technologies in defence &

security. **NATO Review**, 3 jun. 2021. Disponível em: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html. Acesso em: jun. 2024.

WU, Chien Shiung; SHAKNOV, Irving. The angular correlation of scattered annihilation radiation. **Physical Review**, v. 77, n. 1, 1950. DOI: 10.1103/PhysRev.77.136.

XUANZUN, Liu. China's in-development H-20 bomber worth the excitement: PLA Air Force deputy commander. **Global Times**, 11 mar. 2024. Disponível em: https://www.globaltimes.cn/page/202403/1308604.shtml. Acesso em: nov. 2024.

ZHANG, H.; SUN, Z.; QI, R. et al. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. **Light Science & Applications**, v. 11, n. 83, 2022. DOI: 10.1038/s41377-022-00769-w.